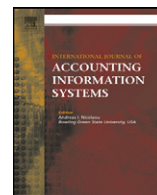




Contents lists available at SciVerse ScienceDirect

International Journal of Accounting Information Systems



A content analysis of auditors' reports on IT internal control weaknesses: The comparative advantages of an automated approach to control weakness identification[☆]

J. Efrim Boritz^{*}, Louise Hayes, Jee-Hae Lim

School of Accounting and Finance, University of Waterloo, Canada

ARTICLE INFO

Article history:

Received 23 November 2011

Accepted 29 November 2011

Keywords:

SOX 404

Information technology control weaknesses

Internal control weaknesses

Content analysis

ABSTRACT

We employ an automated content analysis approach to provide a snapshot of the terminology auditors actually use to describe information technology weaknesses (ITWs). We develop and use a dictionary based on textual analysis of auditors' reports on internal control filed under Section 404 of the Sarbanes–Oxley Act from 2004 to 2009. Using the dictionary with content analysis software led to the identification of 14 categories of ITWs in order of decreasing frequency of occurrence: (1) access, (2) monitoring, (3) design issues, (4) change and development, (5) end-user computing, (6) segregation of incompatible functions, (7) policies, (8) documentation, (9) masterfiles, (10) backup, (11) staffing sufficiency and competency, (12) security (other than over access), (13) outsourcing and (14) operations. The use of automated content analysis methodology also helped us identify potential disconnects between terminology used in auditors' reports and that used in published frameworks and guidelines. We provide the dictionary and discuss the methodology used in creating and applying the dictionary to the analysis of the textual content of auditors' reports on internal control, including the advantages and limitations of automated ITW identification.

© 2011 Elsevier Inc. All rights reserved.

[☆] We wish to acknowledge the funding provided by the Social Science and Humanities Research Council of Canada (SSHRC), the 2009 CAAA/CICA Research Program, the University of Waterloo Centre for Information Integrity and Information Systems Assurance, sponsored by the Canadian Institute of Chartered Accountants, CaseWare IDEA Inc. and ISACA. We gratefully acknowledge the comments of Andreas Nicolaou and four anonymous reviewers and participants at the 2010 Mid-Year Meeting of the Information Systems Section of the American Accounting Association, 2010 Canadian Academic Accounting Association Annual Conference, 2010 European Accounting Association Annual Congress, 2010 American Accounting Association Annual Meeting, and the 2009 University of Waterloo Symposium on Information Integrity and Information Systems Assurance, particularly those of Gary Baker and Ed O'Donnell.

^{*} Corresponding author.

E-mail addresses: jeboritz@uwaterloo.ca (J.E. Boritz), blhayes@uwaterloo.ca (L. Hayes), jh2lim@uwaterloo.ca (J.H. Lim).

1. Introduction

Information technology controls represent a distinct category of internal controls that has been given special attention in professional publications (e.g., COSO and COBIT¹) and auditing standards (e.g., PCAOB Auditing Standard No. 5, 2007). This special attention is warranted because computerized environments are frequently associated with financial misstatements and less reliable financial reporting (Messier et al., 2004; Curtis et al., 2009). Companies reporting information technology weaknesses (ITWs) in reports filed under Section 404 of the Sarbanes–Oxley Act (SOX 404 reports) (SEC, 2003) also report more internal control weaknesses and financial misstatements than companies without ITWs (Klamm and Weidenmier Watson, 2009). To date, the study of detailed ITWs described in SOX 404 reports has been hindered by a number of factors. First, the *Audit Analytics*² database that is relied on by many researchers uses a single code for all ITWs which is not granular enough for delving into specific ITWs. Second, the on-line search tools provided by the SEC to search EDGAR filings are not robust enough to distinguish several common ITWs from other control weaknesses (non-ITWs). As a result, laborious and potentially unreliable manual analysis and coding of the content of auditors' reports are required to identify specific ITWs.

An alternative to manual coding is the use of automated content analysis instead of the arduous, manual processes used by researchers to date. Automated identification of ITWs is consistent (without random human error), replicable (the process is rule-based), scalable (coding efforts are the same regardless of the number of reports analyzed), and transparent (when the keywords/phrases and search criteria used to automate identification are made available). The purpose of this study is three-fold: (1) to compare the efficacy of using automated vs. manual content analysis procedures to identify ITWs in auditors' SOX 404 reports, (2) to provide a categorized dictionary of the terminology auditors most frequently use to report ITWs in SOX 404 reports between 2004 and 2009, and (3) to check whether terminology used in professional frameworks and guidelines is used in auditors' reports on internal control. To accomplish this, we first use frequency, key-word-in-context, and keyword retrieval reporting features of content analysis software to capture and categorize the keywords/phrases actually used by auditors to describe ITWs in SOX 404 reports. Using the categorized dictionary thus developed, we next conduct automated searches of auditors' SOX 404 reports and compared automated identification of ITWs to both our manual coding of all SOX 404 reports from 2004 through 2009 and Klamm and Weidenmier Watson's (2009) manual coding of ITWs in the first year of SOX reporting.

We find that our automated identification compares favorably to the inter-rater manual coding reliability reported by Klamm and Weidenmier Watson (2009). In addition, by examining the keywords/phrases auditors commonly used to describe ITWs in SOX reporting, we identified 14 categories of ITWs using a “bottom up”, inductive approach. These 14 categories of ITWs are, in order of decreasing frequency of occurrence: (1) access, (2) monitoring, (3) design issues, (4) change and development, (5) end-user computing, (6) segregation of incompatible functions, (7) policies, (8) documentation, (9) masterfiles, (10) backup, (11) staffing sufficiency and competency, (12) security (other than over access), (13) outsourcing and (14) operations. In this paper, we illustrate the ease with which these categories may be subdivided and combined, and searches replicated and modified, using automated content analysis techniques. Finally, we use the content analysis software to search the SOX 404 reports in segments in which ITWs are described for the high-level control categories identified in widely-used control frameworks such as COSO and COBIT and Auditing Standards such as the PCAOB's Auditing Standard No. 2 (2004) and Auditing Standard No. 5 (2007). We find that most are not referred to at all and those few that are mentioned appear in only a small number of cases. This represents a potential disconnect between published guidance and actual practice. Any such disconnect may make it difficult for users of the internal control reports to link the reported ITWs back to the professional literature and standards that elucidate likely causes of weaknesses and potential avenues and time horizon for their effective remediation.

This study contributes to the academic and professional literature on internal control both methodologically and by providing a unique analysis of ITWs in SOX reports that was not feasible at this granular

¹ COBIT®. Control Objectives for Information and related Technology (IT Governance Institute., ITGI, 2007) outlines good practices that fit with and support the COSO framework.

² The *Audit Analytics* database indicates that 22% of the SOX 404 reports with internal control weaknesses for 2004–2009 year-ends had weaknesses related to the single code defined as information technology, software, security, and access issues.

level in past research due to methodological constraints. By explaining and illustrating the use of automated content analysis, this study contributes to a better understanding of the approach's advantages and limitations and helps researchers decide when an automated approach to content analysis may be preferred to a manual approach. Our automated approach differs from the manual approach used in previous studies (e.g., Hammersley et al., 2008; Klamm and Weidenmier Watson, 2009) in that detailed ITWs are studied without imposing any conventionally used control framework, such as the COSO framework.³ New insights into both the types of ITWs reported by auditors and the frequency with which they are reported are gained from our automated content analysis.

Researchers, hampered by the lacking granularity of the coding of ITWs in the *Audit Analytics* research database, will find that this content analysis approach allows for more functional querying capabilities than the online search tools provided by the SEC to search EDGAR filings. Researchers may need a tool for sub-dividing the single code for all IT weaknesses that is used in *Audit Analytics* into sub-codes to test the robustness of results. Our 14 categories, being defined at a more detailed level of granularity than the groupings commonly used in professional standards and other guidance such as the COSO framework, may lead to a more nuanced understanding of ITW effects. Also, the “dictionary” of words/phrases created in this study (Table 1) to identify and categorize reported ITWs may assist management and auditors in the reporting of ITWs in future SOX 404 reports and other contexts (e.g., management discussion and analysis). Our finding of a potential disconnect between published guidance and actual practice suggests the need for either revisions to guidance or elaboration of descriptions of framework(s) used in SOX 404 ITW reporting.

This paper is structured into five sections. After the [Introduction](#), the second section provides a review of existing research and develops two research questions. The third section outlines the data sources and methods employed in this study while the fourth presents and discusses the findings arising from the analyses conducted to address our research questions. The final section summarizes the contributions of this research, discusses its limitations, and identifies opportunities for future research.

2. Literature review and research question development

The use of automated content analysis and other text analytics methodologies in accounting research has grown exponentially over the last five decades (Fisher et al., 2010). However, such methods have not been used for ITW identification. The automated search capabilities of qualitative data analysis and text analytics software vary and “nomenclature confusion” surrounds content analysis (Pollach, 2011). We distinguish manual content analysis, computer-assisted content analysis, automated content analysis, and more advanced text analytics not by the type of software used but rather by the ways in which automation is used to leverage research expertise. Whenever researchers manually read text to code the constructs of research interest we consider content analysis either “manual”, when office productivity or statistical analysis software is used to record codes, or “computer-assisted”, when use of qualitative data analysis software is limited to assisting with text management, coding, and text retrieval. Humans are very good at understanding unstructured text. However, humans also make mistakes, grow fatigued, and bring varying training, experience, and time constraints to text coding tasks. Accordingly, when software is used only to assist with content analysis, coding may be inconsistent and may not be completed within time and budget constraints.

Categorized dictionaries, lists of keywords/phrases linked to concepts, and explicit, sometimes complex, search rules make automated content analysis of unstructured text possible. Once researchers make the upfront investment in dictionary development, increasing numbers of documents may be analyzed with little additional effort. When shared, the categorized dictionary and search rules make construct identification with automated content analysis transparent and replicable.⁴ Qualitative data analysis software typically comes

³ SOX 404 requires management and auditors to identify the framework used to assess the effectiveness of internal control over financial reporting. The framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) is the one most frequently used (Gupta, 2006).

⁴ While researchers conducting manual text analyses may also list the explicit search rules used and the words/phrases linked to constructs, such lists are unlikely to be complete when a manual approach is adopted.

Table 1Frequency of reporting of keywords/phrases in the dictionary used in automated content analysis of SOX 404 reports with ITWs^a.

	Keyword(s)/phrases ^a
IT context indicator keywords and phrases which are not associated with a specific ITW category	information technology (161); user* (51); software (48); accounting system* (43); information system* (43); financial application* (42); automated (34); computer* (28); financial application programs and data (24); database* (21); comput* (20); reporting system* (17); payroll process* (16); ERP (15); IT general controls (13); system* control* (9); billing system* (8); network (8); inventory process* (7); financial reporting system (6); general ledger system* (6) perpetual inventory records (6); enterprise resource planning (5); inventory system* (4); Oracle (4); platform* (4); processing of financial data (4); system-generated report* (4); computing (3); data entry (3); ITC* (3); ITGC (3); online (3); accounts payable system* (2); application source code (2); application system (2); billing process* (2); computer-generated (2); inventory costing system* (2); IT controls (2); IT department (2); IT function (2); payroll system* (2); point-of-sale (2); processing file* (2); SAP (2); transactional control* (2); accurately enter* (1); application based (1); CIO (1); current system (1); data processing (1); enterprise business system (1); enterprise resource platform (1); financial accounting IT applications (1); financial software system (1); financial system application* (1); generated by the system (1); hardware (1); input* to model* (1) IT staff* (1); IT support staff (1); Microsoft AX (1); model input* (1); MRP (1); operating system (1); programmer* (1)
IT weakness (ITWs) categories	
<i>Keywords/phrase in bold font type are also IT context indicator keywords/phrases^a</i>	
Access	access (168); user access (40); access control* (33); restrict* access (30); password* (18); system access (16); inappropriate access (14); access rights (9); logical access (9); security access (8); access privilege* (4); physical access (3); security setting (3); system right* (2); network access (1); prevent management override (1); system privile* (1); user identification (1)
Monitoring	oversight (384); review* (258); monitor* (185); supervis* (126); examin* (73); logging (4); scrutiny (1)
Design issues	design* (387); reporting requirement* (50); complexit* (23); lack of effective (19); assumption*used (11); formal process* (9); manual process* (8); inadequate system* (7); legacy (6); manual intervention* (6); disparate (5); manually (5); decentralized (4); interface* (4); not integrated (4); incompatible application* (3); lack of a unified (3); non-integrated (3); audit trail* (2); manual performance (2); do not appropriately address the requirements (1); functional business requirement* (1); inadequate recording and report* (1); invest sufficiently in technology (1); large number of manual process* (1); manual* intensive* (1); over-reliance on (1); properly integrated (1); reporting capabilities (1); reporting limitations (1); system capabilities (1); user dependence (1)
Change and development	test* (385); implementation (46); change management (37); development (35); program change* (23); program development (16); configure* (15); change control* (11); conversion (10); migrat* (9); system change* (7); changes to financial (5); system* development (5); version control (5); approval of chang* (4); accuracy of calculat* (3); system* conversion* (3); authorized change* (2); changes to production application* (2); placed into production (2); program* error* (2); project management (2); set-up (2); software chang* (2); application error* (1); authorization of chang* (1); changes to program* (1); deactivat* (1); develop and validate (1); maintenance control* (1); recording changes (1); testing of program chang* (1); track* chang* (1); updated and maintained (1)
End-user computing	spreadsheet* (119); end-user comput* (11); end user comput* (4); user developed application (2); cell protection (1)
Segregation of incompatible functions	segregat* (182); incompatible duties (17); incompatible responsibilit* (2);

(continued on next page)

Table 1 (continued)

	Keyword(s)/phrases ^a
Policies	policies (387); policy (42); lack of documented procedures (1)
Documentation	document* (174)
Masterfiles	master file* (23); payroll changes (7); census data (4); data file* (4); master data (4); payroll data (4); vendor data (3); vendor management (3); master record* (2); masterfile* (2); master-file* (2); vendor setup (2); vendor set-up (2); price table* (1); standing data (1); vendor accounts (1); vendor file* (1); vendor listing (1) train* (113); experienc* (80); knowledg* (74); *sufficient complement of personnel (40); *sufficient number of (24); *sufficient personnel (24); skill* (21); inadequate staff* (10); competenc* (5); adequate staffing (3); *sufficient complement of staff (3); understaffed (3); inadequate IT staff (2); inadequate personnel (2); inadequate IT support staff (1); limited number of personnel (1); personnel limitation* (1); shortage of resources (1); turnover of personnel (1); backup* (13); disaster (9); back-up* (8); offsite (6); back up* (5); off-site (3); record* storage (1); remote location (1); removable media (1); rotation media (1); uninterruptible power (1)
Staffing sufficiency and competency	computer operation* (11); information system* operation* (3); software licens* (3); IT operation* (2); operating procedure* (2); operations report* (1)
Backup	physical security (7); information security (5); it security (4); encrypt* (3); firewall (3); security management (3); security setting (3); control* over security (2); security and data protection (2); security issue* (2); system security (2) antivirus (1); anti-virus (1); electronic transmission (1); fire (1); intrusion detection (1); network vulnerability assessment* (1); security breach (1); security configuration (1); security incident* (1)
Operations	service provider* (14); outsourc* (7); SAS 70 (3); third-party service (3); data center* (1); out-sourc* (2);
Security (other than access)	
Outsourcing	

^a Keywords/phrases in the dictionary used to search for IT weakness indicators near (in the same sentence and within 20 words either side) of IT indicators. IT indicators keywords/phrases are shown in bold font. Less restrictive searches reported in Table 3, were conducted for IT weakness indicators anywhere in sentences that contain IT indicators. In more restrictive searches reported in Table 3, ITWs are ignored if also within 20 words (as determined by the content analysis software) of “exclusion keyword/phrases” in sentences with IT indicators. Exclusion keyword(s)/phras(es), frequently associated with SOX 404 “boilerplate” definitions and non-ITW contexts are: adherence to policies; capitalization polic*; capitalized software; communicat* policies; communication to employees; compliance with; corporate governance policies; costs of computer software; do not execute; did not operate effectively; documentation regarding; documentation supporting; enforce; enforcement of; ensure the proper operation; established company policies; execute its policies; failed to apply; four aspects of information technology general controls; four basic information technology; four basic IT; in accordance with; information technology area*; information technology controls are policies; internally developed software; IT areas; ITCS are policies; ITCS include four basic; multiple element software arrangement*; policies did not operate effectively; revenue recognition polic*; software accounting policies; software capitalization; software development costs; source document*; sufficiently document; support operations; supporting documentation; the company’s polic*; the policy of; and were not followed.

with tools (word frequency count, key-word-in-context, similarity measure, text extraction, and drag and drop categorization tools) to help the researcher group keywords/phrases into categories. However, coding may be unreliable and insufficiently grounded in theory if categories are formed using automated text mining without someone with subject matter expertise reviewing and refining the linkages. While today’s automated content analysis toolkits have sophisticated data visualization, mapping, and networking tools, expert categorization and search rule development will continue to distinguish automated content analysis from other text analytics methodologies. Fig. 1 summarizes the software features necessary and the expertise leveraged along the content analysis/text analytics spectrum.

Using automated content analysis to study ITWs in SOX 404 reports presents a unique opportunity for comparing the efficacy of manual vs. automated content analysis of unstructured text. There are several hundred SOX 404 reports in which auditors describe ITWs in unstructured text: a number sufficient for development and validation of the categorized dictionary of keywords/phrases required for automated content analysis. Further, there exists a manual/computer assisted content analysis of ITWs (Klamm and Weidenmier Watson, 2009) to which the results of the automated search may be compared. Since recent

Content Analysis Approaches using Qualitative Data Analysis (QDA) Software

	Content Analysis in Accounting Research			Additional Text Analytics Tools
	Manual	Computer Assisted	Automated	
Qualitative data analysis (QDA) software features	n/a	<ul style="list-style-type: none"> - import and manage documents - point-and-click or drop and drag coding -marginal code display -coding history (coder, dates) -report inter-rater agreement - retrieve coded text - query and search text 	computer assisted content analysis functionality plus: <ul style="list-style-type: none"> -advanced dictionary building support (e.g., word frequency and keyword-in-context reporting; similarity and dispersion reports and visualization tools; drop and drag dictionary creation tools) - advanced Boolean and proximity search capabilities - automated coding 	automated content analysis functionality plus: <ul style="list-style-type: none"> -natural language processing - advanced statistical and/or linguistic tools - fuzzy logic to better handle text variants
Coding	manual approach: <ul style="list-style-type: none"> - experts read reports and record coding in spreadsheet or statistical software 	manual approach: <ul style="list-style-type: none"> - experts read reports stored in QDA software and apply codes to selected text -codes are exported for subsequent analysis 	hybrid approach: <ul style="list-style-type: none"> - experts create “dictionaries”, i.e., keyword/phrase lists categorized by concepts of interest - QDA software searches text and codes sentences or paragraphs when the text matches a keyword/phrase in the category -software tools (e.g., word frequency and keyword-in-context reports) are used to develop wordlists and dictionaries 	text mining approach: <ul style="list-style-type: none"> - sophisticated tools for concept linking and dictionary creation - dictionary creation remains an iterative process refined by expert decisions on categorization and use of linguistic resources
Coding changes	<ul style="list-style-type: none"> -experts reread and recode reports 	<ul style="list-style-type: none"> - experts reread and recode text -code reporting may aid in locating text segments requiring checking or change 	<ul style="list-style-type: none"> -experts change dictionary or search criteria - automated coding process is rerun -text retrieval may be used in conjunction with less sophisticated dictionaries to locate segments of text for further manual analysis 	<ul style="list-style-type: none"> - advanced text analytics is an iterative process: recoding following refinement of categories is part of dictionary building
Advantages	<ul style="list-style-type: none"> - expert coding is reliable and inexpensive for a small number of documents 	<ul style="list-style-type: none"> - expert coding of unstructured text is more reliable than automated coding, time permitting - investment in costly dictionary creation is avoided -facilitates inter-rater agreement and coding changes 	<ul style="list-style-type: none"> - consistent, scalable, and replicable text coding - transparent search rules via re-usable keywords/phrases in categorized dictionaries - expertise is leveraged and coding is grounded in theory through expert involvement in dictionary creation - relationships may be discovered during “bottom-up”, inductive, dictionary creation process 	<ul style="list-style-type: none"> - sophisticated software for handling relational complexities and semantic ambiguities of unstructured text - cost saving from investing in sophisticated tools increases as the number of documents grows large

Fig. 1. Content analysis approaches using qualitative data analysis (QDA) software.

research has shown significant associations between the presence of ITWs and variables of interest in many streams of accounting literature,⁵ the study of specific ITWs driving such associations will be facilitated by a development of an automated approach for identification of specific ITWs.

Auditors' ITW descriptions are embedded in lengthy, detailed unstructured text descriptions of internal controls over financial reporting such as in SOX 404 reports. Developing automated procedures to search this type of unstructured text presents coding challenges. SOX 404 reports are available through the Security and Exchange Commission's (SEC's) EDGAR system or more conveniently through the *Audit Analytics* database. *Audit Analytics* uses 21 codes to code reports containing internal control weaknesses, but only one code is used to identify reports containing any ITWs. Thus, accounting researchers interested in studying detailed ITWs may use the *Audit Analytics* database to locate SOX 404 reports with ITWs but must then analyze the content of these reports to identify and code individual ITWs.⁶ A special challenge for automating identification of ITWs is that auditors use similar language to describe non-ITWs and ITWs. Thus, complex search approaches are required that not only search for specified keywords/phrases but also search for information technology references in nearby context to distinguish ITWs and non-ITWs described with the same keywords/phrases (e.g. lack of training and segregation of incompatible duties). Fig. 2 illustrates this challenge with segments from several actual SOX 404 auditors' reports.

Another challenge for automated content analysis identification of ITWs is that a specialized dictionary of keywords/phrases associated with ITWs has not been previously developed nor are ITWs categorized the same in all professional guidance. Content analysis software requires a specialized "dictionary" of keywords/phrases, categorized into predefined groups that identify the main themes to identify ITWs in SOX 404 reports. Internal control frameworks and guidelines (e.g., COSO) and auditing publications (e.g., PCAOB Auditing Standard No. 5, 2007) discuss the distinction between various categories of IT controls such as Application Controls, General Controls, and sub-categories such as the subdivision of General Controls into Operations Controls, System Development and Maintenance Controls, and Security Controls. Thus these categories may seem like natural choices for the keyword dictionary. However, Hunton's (2000, p. 33) admonition that "a framework can lead us to believe that the framework is the world and this can inhibit our ability to think outside the box" suggests that categorization should reflect the keywords/phrases used by auditors to describe ITWs. While content analysis software with word frequency counts and key-word-in-context reporting capabilities facilitates such "dictionary" development, keywords/phrases categorization is a manual process and categorization errors and omissions may affect ITW identification reliability. This leads to our first research question:

RQ1: Is automated content analysis identification of ITWs in auditors' SOX 404 reports as reliable as manual content analysis identification?

The use of an automated content analysis approach not only contributes to the consistency, replicability, scalability and transparency of ITW identification, but also facilitates study of how well various categorizations of keywords/phrases capture auditors' reporting of ITWs. However, due to the lack or non-consensus of guidance for ITWs, previous studies have used different categorizations for ITWs. For example, Klammm and Weidenmier Watson (2009) identify 12 material ITWs and group these by the five components of the COSO framework (control environment, risk assessment, control activities, information and communication and monitoring). Li et al. (forthcoming) and Masli et al. (2009) group 25 ITWs into seven categories (access controls, enterprise architecture, general IS/IT controls, IT capabilities, security and recovery, application

⁵ In previous research, using the *Audit Analytics* database or the *Compliance Week* information service (now discontinued) researchers have found weak IT control associated with non-ITWs (Klammm and Weidenmier Watson, 2009), audit fees (Raghunandan and Rama, 2006; Hoitash et al., 2008; Canada et al., 2009), audit committee quality (Krishnan, 2005), financial performance (Boritz and Lim, 2008), earnings management and accruals (Doyle et al., 2007b; Ashbaugh-Skaife et al., 2008; Cohen et al., 2008), stock price and cost of capital reactions to the disclosures of internal control weaknesses (Beneish et al., 2008; Hammersley et al., 2008; Ashbaugh-Skaife et al., 2009), and performance-based executive compensation (Jha et al., 2010; Hoitash et al., forthcoming).

⁶ The SEC provides online search tools to search corporate filings on EDGAR; however, these are not sufficient for identifying all ITWs in SOX 404 reports. The SEC-supported search options do not permit restricting keyword/phrase searches to a sentence or checking content near search terms (http://www.sec.gov/edgar/searchedgar/search_help.htm). Such features are necessary to avoid false identification of ITWs (Type 1 errors) or omission of ITWs (Type 2 errors).

Examples of Information Technology Weaknesses (ITWs) Reporting in SOX 404 Internal Control Reports^a

Documentation, Policy, Monitoring, Backup, and Operations weaknesses example:

“These [and other] deficiencies in the aggregate represented more than a remote likelihood that a material misstatement of the Company's annual or interim financial statements would not have been prevented or detected.... Deficiencies related to **backup** tape *off-site* storage, **backup** tape on-site storage, **monitoring** of **backups**, problem management, periodic restoration of **backups**, **backup** tape rotation **policy**, **backup** tape log, completion of job schedules, **documentation** of **operating procedures**, and **operations reporting**.” Modtech Holdings Inc., 2004

Monitoring and Access weaknesses example^b:

“Specifically, ineffective controls included unrestricted **access** for *information technology* and accounting personnel to programs and data, the lack of periodic, independent **review** and **monitoring** of such **access**, and a lack of **policies** and procedures that govern security and **access**.” Adelphia Communications Corp, 2004

Design and Staffing sufficiency and competency weaknesses example:

“The Company's *information systems* were inadequate to support the **complexity** described above due to multiple, **incompatible applications** and *platforms*, manual *interfaces* and **inadequate IT support staff**.” Sun-Times Media Group Inc., 2004

Security (other than over access), End-user computing and Change and development weaknesses example:

“The Company has also identified *information technology* control weaknesses in the areas of **information security**, **end-user computing**, systems program **development** and **change controls**.” American Apparel, 2008

Access, and Masterfiles weaknesses example:

“Inadequate **access** controls with regard to computer **master files** information - Certain of the Company's personnel in accounts payable and accounts receivable had **access** and could make changes to **master files** without approval.” Parlux Fragrances Inc. 2007

Outsourcing, Change and development and Documentation weaknesses example:

“The Company did not maintain effective controls over certain independent **service providers**. Specifically, the Company was unable to **document**, **test**, and evaluate controls at third party vendors to which the Company **outsources** certain *payroll processing* services in North America.” Interpublic Group of Companies 2005

Segregation of incompatible functions weakness example:

“The Company did not maintain effective **segregation** of duties over *automated* and manual transaction processes.” Dana Holding Corp. 2005

Fig. 2. Examples of information technology weaknesses (ITWs) reporting in SOX 404 internal control reports^a.

^aAutomated searches locate sentences in SOX 404 Auditors' reports that contain both an *IT indicator* (keywords/phrases related to IT hardware, software, procedures and personnel such as the italicized words in the examples above) and a **weakness indicator** (such as the words formatted in bold in the examples above). The approximately 200 weakness identifiers are categorized into the 14 categories of IT weaknesses listed in Table 1.

^bA policy weakness was not identified as the processing rule that was used restricted searches for keywords (e.g. policies) to a range of 20 words on either side of specified IT indicator keywords or phrases (keywords/phrases related to IT hardware, software, procedures and personnel such as the italicized words in the examples above) in the same sentence as IT indicators.

controls and application development) according to common professional practice.⁷ Still other researchers (e.g., Doyle et al., 2007a) group ITWs with other company-wide control weaknesses on the assumption that ITWs have a pervasive, company-wide effect (Canada et al., 2009). Therefore, through modifying the dictionary and categorization used for automated content analysis, our second research question proposes to

⁷ Masterfile, inadequate IT staffing and undue reliance on manual processes would be mapped to “control activities” under COSO whereas, Li et al. (forthcoming) and Masli et al. (2009) would likely map them respectively to application controls, IT capabilities and enterprise architecture categories.

study frameworks used by auditors in preparing SOX 404 reports to be used in conjunction with content analysis software to address the following research question:

RQ2: What are the most common IT control weaknesses reported in auditors' SOX 404 reports and what terminology do auditors choose to describe them?

3. Data sources and methodology

We used a four-step process (described below) to automate ITW identification without imposing terminology drawn from textbooks, professional guidelines and standards: 1) prepare SOX 404 reports for automated content analysis; 2) develop a dictionary and search criteria; 3) assign weaknesses to categories; and 4) validate the identification process.

3.1. Step1: preparing SOX 404 reports for automated content analysis

We gathered 471 SOX 404 auditors' reports on Internal Controls over Financial Reporting from the *Audit Analytics* database of the first six years of SOX reporting (2004–2009). The *Audit Analytics* database obtained these reports from companies' Form 10-K and 8-K SEC filings. These reports were coded as “IT weak” under the single code “Information technology, software, security and access issue” available in the *Audit Analytics* database. We supplemented the *Audit Analytics* database with 6 additional reports identified by Boritz and Lim (2008) through a manual coding of all 2004–2006 adverse SOX 404 reports in the *Audit Analytics* database. We imported these 477 reports into QDA Miner 3.0.4, the qualitative data analysis software from Provalis Research we used to manage the SOX 404 text and manually code ITWs for our comparative analysis. Of the many available qualitative data analysis software products available⁸ we selected QDA Miner 3.0.4 and WordStat v5.1, the software from Provalis Research that provides the word frequency, keyword-in-context, and other dictionary building tools for an automated content analysis approach, as WordStat supports the multiple-category Boolean search and drop and drag multi-level categorization features we used to investigate our research questions.

3.2. Step 2: developing the dictionary and search criteria

Using frequency reporting (Lacity and Janson, 1994) and key-word-in-context (KWIC) features (Fan et al., 2006) of WordStat v5.1, we developed the “dictionary” used for the automated search. First, we produced a frequency report showing all words and their frequency in all the SOX 404 auditor's reports. We began creating a new dictionary for our study by entering the keywords from this frequency report with over 5000 words, that referred to ITWs directly (e.g. password) or words likely to be in a segment of the SOX 404 report in which an ITW might be described (e.g. technology). As we entered the keywords into the dictionary, we categorized the entries as “IT indicators”, using subcategories (which we could change at any time) within the “IT indicator” category to help organize the dictionary. Next, we used the KWIC feature to display reports of words/phrases near these IT indicators that auditors used to describe ITWs. Since ITW weaknesses are described in the reports but strengths are not, keywords such as “training” or “change management” could often be used in the dictionary without modifiers such as “lack of” or “inadequate”. We entered the keywords/phrases used by auditors to describe ITWs as “weakness indicator” words/phrases in other categories of the dictionary, cognizant that the categorization would be revisited as dictionary building progressed. Fig. 3 shows frequency and KWIC reporting and Fig. 4 is a screenshot of a portion of the dictionary building screen.

Search rules, developed to identify ITWs while avoiding erroneously identifying ITWs in boilerplate wording describing management and auditor reporting responsibilities and to avoid wrongly counting non-ITWs as ITWs when they share similar descriptions (e.g., “lack of training”, and “insufficient staffing”),

⁸ The “resources” page of the website for the University of Surrey's Computer Assisted Qualitative Data Analysis Networking Project includes links to qualitative data analysis products and information on selecting software. <http://www.surrey.ac.uk/sociology/research/researchcentres/caqdas/>. Pollach (2011) also compares the features of several products.

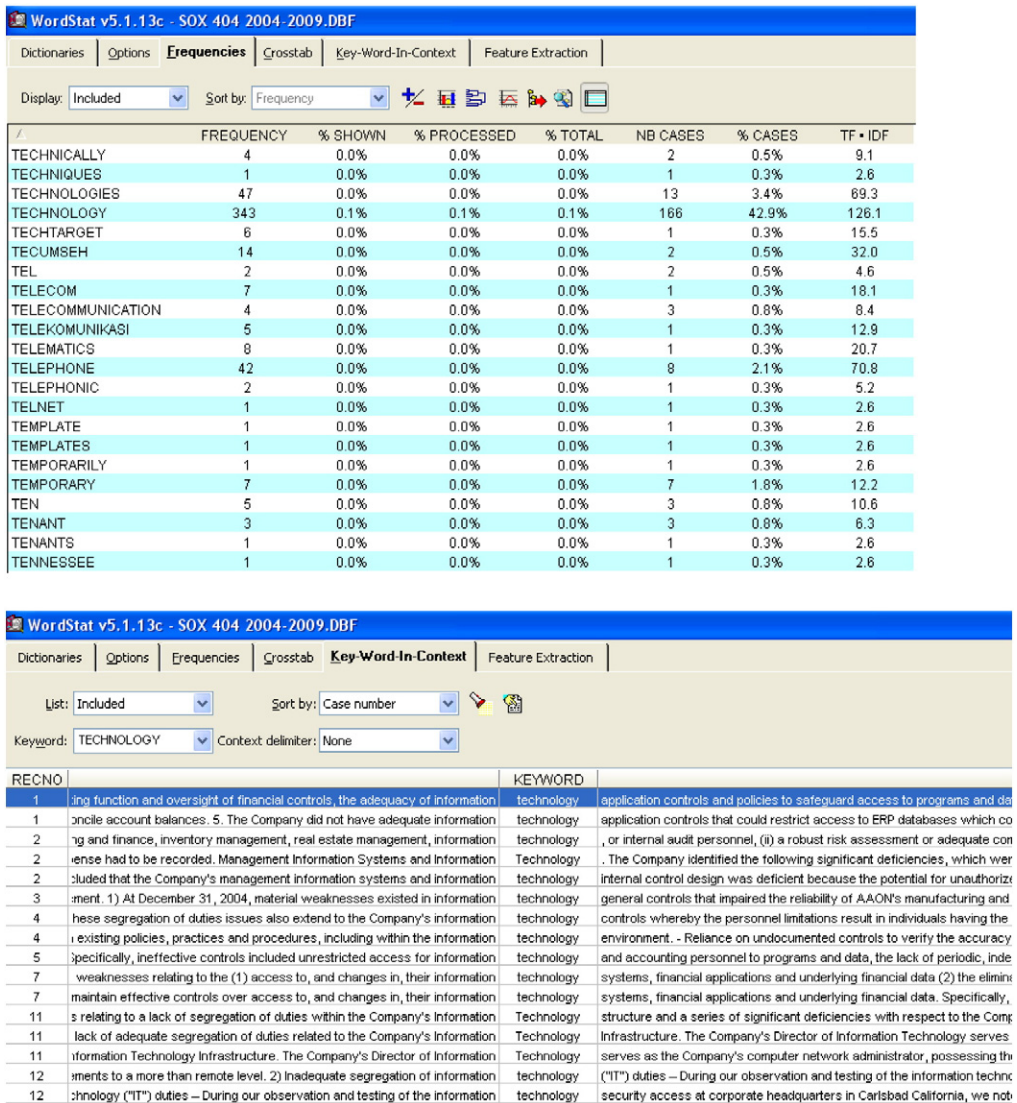


Fig. 3. Word frequency and key-word-in-context reports from WordStat v5.1.

were added to the dictionary. Search rules programmed the automated content analysis to search for both an *IT indicator* (keywords/phrases related to IT hardware, software, procedures and personnel) and a *weakness indicator* in the same sentence (keywords/phrases, together with wildcard character “*” usage, allowing for variation in keyword endings, related to the specific nature of the ITW such as “monitor”, “monitor*”, “access”, “change management”, and “masterfile”). Wordstat v5.1 shows the number of reports identified by each search rule as part of frequency reporting and automatically reruns all searches whenever a change is made to the dictionary and a frequency report displayed. We repeatedly used the keyword retrieval feature of the software to “drill down” from these updated search results and examine the sentences describing ITWs (some of which were “false hits” and some of which included other ITWs not yet found by the automated searches) to refine the dictionary. Fig. 5 shows a portion of a keyword retrieval report.

Iteratively, we refined the keywords, modified the search criteria (to search for *IT weakness indicators* within a specified number of words of *IT indicators* within sentences with *IT indicators*) upon reviewing

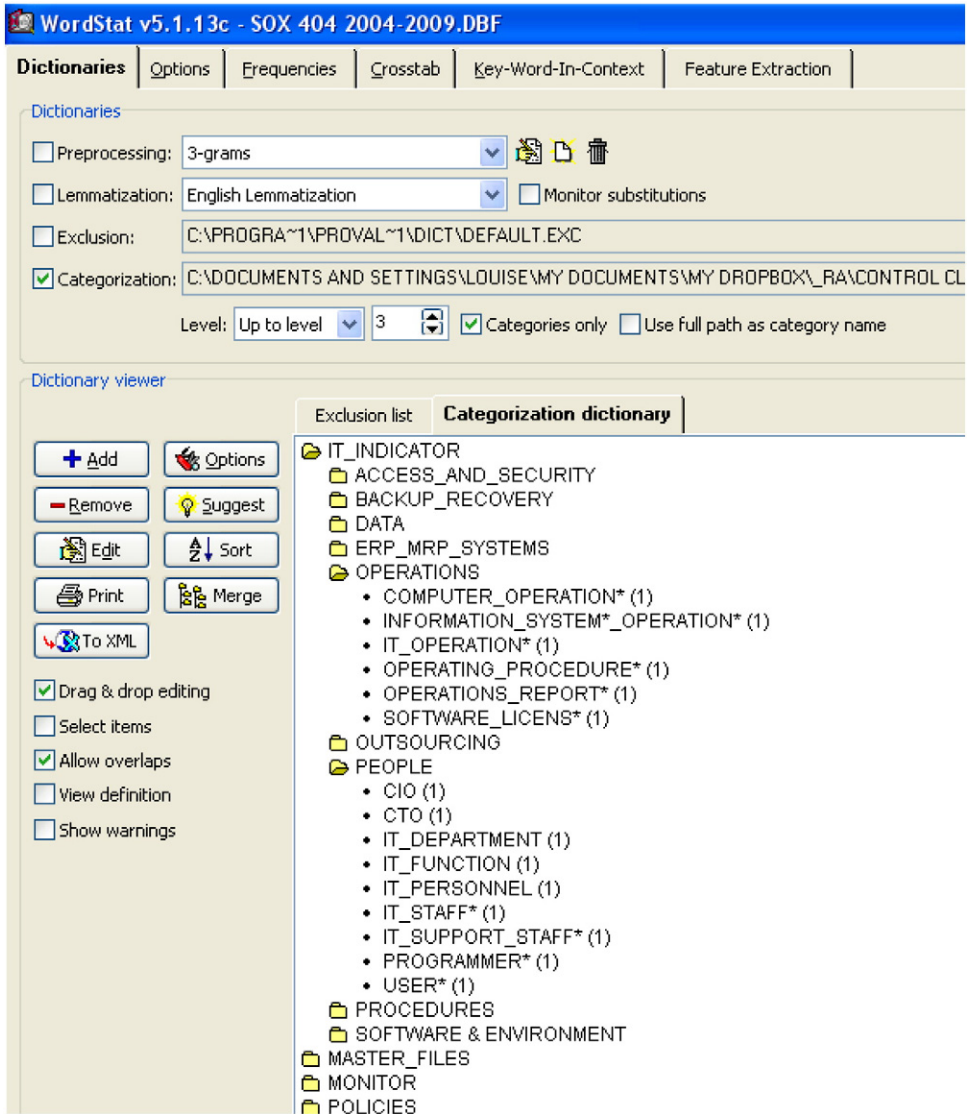


Fig. 4. A portion of the categorization dictionary screen.

updated frequency, KWIC, and retrieval reports. Our objective was not to optimize the dictionary and search criteria, but rather to compare the reliability of an automated content analysis approach to a manual one and to produce a dictionary that makes our content analysis approach transparent and replicable. Dictionary development is a time consuming process without an objective “stopping rule”. We moved to step 3, when diminishing returns of improved search results no longer balanced further effort in refining the dictionary and search strategies.

3.3. Step 3: assignment of keywords/phrases to categories

Recognizing that the IT weakness categories are the main constructs in our ITW investigation we revisited the categorizations, the identification of the main themes (Fan et al., 2006), we had used to organize

Keyword Retrieval		
Criterion	Results	
CODE:	<input type="text"/>	<input checked="" type="checkbox"/> Multilines grid
Case #	Text	FILE
1	3D SYSTEMS CORP10-K 2006 Auditor - Internal Control OpinionREPORT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRMTTo the Stockholders and Board of Directors of 3D Systems Corporation Rock Hill, South CarolinaWe have audited management's assessment, included in the accompanying Management's Report on Internal Control Over Financial Reporting appearing in Item 9A of the Annual Report on Form 10-K, that 3D Systems Corporation and its subsidiaries (the "Company") did not maintain effective internal control over financial reporting as of December 31, 2006 because of the effect of material	129 3D SYSTEMS CORP 06
1	The Company did not maintain adequate controls over financial SPREADSHEETS that are part of the financial statement preparation process.	129 3D SYSTEMS CORP 06
5	Specifically, the Company had (i) ineffective controls over the DOCUMENTATION , authorization and REVIEW of journal entries; (ii) ineffective controls to ensure the accuracy of and restricted ACCESS to SPREADSHEETS used to support journal entries reflected in the Company's general ledger and in its financial reporting process, and (iii) ineffective controls to ensure the completeness of certain general ledger account reconciliations conducted in connection with the period-end financial reporting process.	71 ADELPHIA COMMUNICATIONS CORP 04
13	• A series of significant deficiencies were noted in the Company's system of internal control over financial reporting including: lack of audits of ceding company data, OVER-RELIANCE ON SPREADSHEETS , and OVER-RELIANCE ON analytics as preventive controls.	186 ANNUITY & LIFE RE 04
19	Ineffective REVIEW of Account Analyses The Company did not have POLICIES and procedures to ensure adequate REVIEW of all significant account analyses and SPREADSHEETS used to record journal entries.	201 AUDIBLE INC 06
24	Deficiencies in end-user COMPUTING controls.	63 BALLY TOTAL FITNESS HOLDING CORP 04
24	The Company did not maintain adequate controls over end-user COMPUTING .	63 BALLY TOTAL FITNESS HOLDING CORP 04

Fig. 5. Keyword retrieval report showing sentences identified by search rule used to identify end-user computing ITWs.

the dictionary before commencing dictionary validation. We printed out the dictionary and agreed on the categories chosen and the category assignment of keywords/phrases. While we were guided by theory in our discussion, in some instances the final categories were more multi-dimensional than theory would dictate due to the infrequent occurrence of words/phrases. For example, given less than 40 reports of staffing insufficiency, lack of experience and training, we used a single multidimensional category for staffing and competency.

We grouped the approximately 200 keywords/phrases used by auditors in ITW SOX 404 reporting into 14 categories using a "bottom up", inductive approach, trying to maximize the number of categories to preserve distinctions while ensuring there were enough reports in each category to permit subsequent statistical analyses. Fig. 6 shows examples of the dendrogram and concept mapping visualization features of the software we used, along with statistical correlation analysis, to assess the discriminant validity of

the 14 categories. For example, as shown in Fig. 6, when the number of clusters⁹ is set to 11, the concept mapping tool uses similarity analysis to combine End-user computing and Design ITWs into one cluster and Access, Monitoring, and Segregation ITWs into another cluster to reduce the 14 categories of ITWs into 11 categories, mapped using 11 different colors. The dendrograms and concept mappings helped us visualize the instability of ITW clustering under different similarity indices and confirm our decision to retain all 14 categories in the dictionary.

3.4. Step 4: validating dictionary and search criteria

To validate the dictionary and search logic developed in step 3, we followed two validation approaches: The first approach involved a review of the categorization dictionary by two senior audit partners from two different Big 4 firms who each have had considerable (over 20 years) IT governance and control assurance expertise. Secondly, one of the researchers and a graduate student collaboratively performed a manual coding of ITWs. Fig. 7, a screenshot of QDA Miner, shows computer-assisted ITW coding used during the manual coding procedure.

We then compared the software-based automated ITW identification to the researchers' manual coding. Since the quality of unstructured text acquisition and analysis can be altered dramatically through small changes in dictionaries and processing rules (Kuechler, 2007), we applied varying search rules to test the sensitivity of search results to our rule choice. We computed the Type 1 errors (false hits), Type 2 errors (misses) and ITW identification agreement as percentages of the ITW identified with the manual approach.

3.5. Further analysis

To investigate our first research question (*Is automated content analysis identification of ITWs in auditors' SOX 404 reports as reliable as manual content analysis identification?*) we compared ITW identification using the validated automated content analysis approach to the frequency of ITW reporting reported by Klamm and Weidenmier Watson (2009). Klamm and Weidenmier Watson (2009) read and coded 490 SOX 404 reports and reported the frequency of occurrence of 12 detailed ITWs in the first year of SOX reporting, the time period of their study. For this comparison, we limited our automated search to the first year of SOX reporting and used the search criteria that balanced failure to identify ITWs (Type II errors) against false identification of ITWs (Type I errors). The ITW frequency reporting used in the investigation of RQ1 was also used to investigate our second research question, "*What are the most common IT control weaknesses reported in auditors' SOX 404 reports and what terminology do auditors choose to describe them?*"

4. Results

In Table 1 we present the search rules and the keywords/phrases in the categorized dictionary we developed to automate the identification of ITWs in auditors' SOX 404 reports. Before comparing the reliability of automated vs. manual ITW identification (RQ1), we discuss observations during the four step process of developing the categorized dictionary presented in Table 1.

4.1. Result of step 1: preparing SOX 404 reports for automated content analysis

We initially imported 477 reports into QDA Miner 3.0.4. However, we revisited this step and deleted 90 of these reports following subsequent automated content analysis (see step 4 below) which failed to find ITWs in 118 reports in automated searches for any IT weakness indicator keywords/phrases in sentences containing IT indicators. We found *Audit Analytics* coded 90 of these 118 reports as ITW weak based on the wording in *management's* SOX 404 report, whereas the corresponding wording in *auditors'* reports did not describe ITWs. Since we restricted our study to the *auditors'* SOX reports, we omitted

⁹ Clustering groups similar documents "on the fly" based on text analytics instead of through predefined topics (Fan et al., 2006, 79).

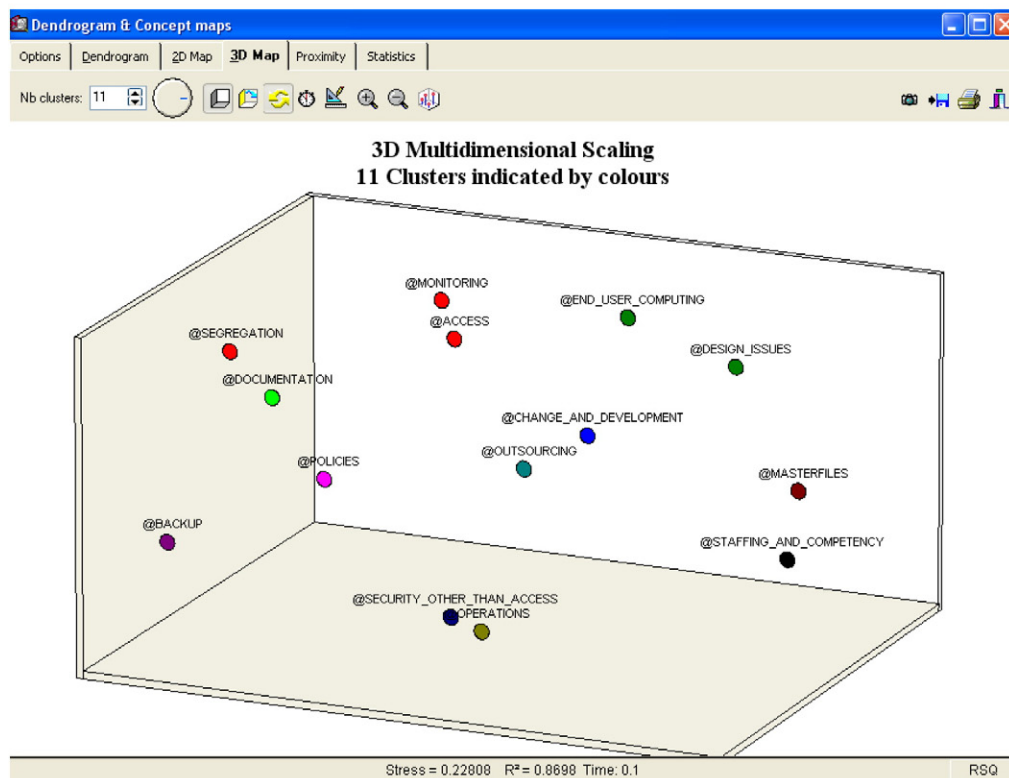
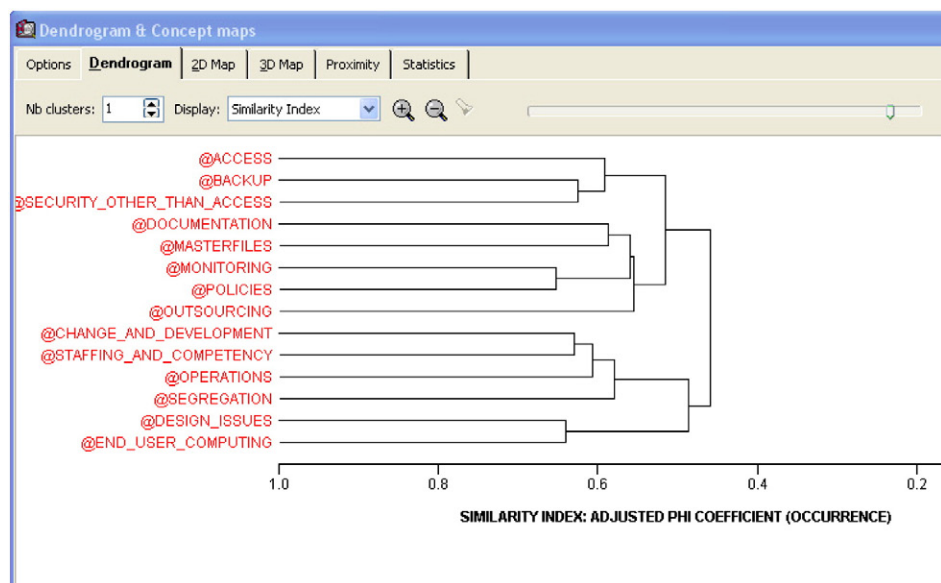


Fig. 6. Dendrogram and 3D visualization of category similarity.

Project Cases Variables Codes Document Analyze Help

CASES:

- 293 MUNICIPAL MORTGAGE 06
- 294 NATURES SUNSHINE PRODUCTS INC 06
- 295 STAAR SURGICAL CO 06
- 296 Voyager Learning CO 06
- 300 ADVANCED ENVIRONMENTAL RECYCLING TECHNOLOGIES INC 07
- 301 ADVANCED OXYGEN TECHNOLOGIES INC 07
- ▶ 303 AMERICAN APPAREL 08

VARIABLES

- FILE 303 AMERICAN APPAREL 08

DOCUMENT [DOCUMENT]

CODES

- ITweaknesses
 - 1_00_01_IT_sentence
 - 1_01_01_monitoring
 - 1_01_02_review
 - 1_02_01_IT_personnel_not_segreated
 - 1_02_02_Other_IT_Segregation_Issues
 - 1_03_01_user_segregation_not_system_implements
 - 1_03_02_ability_to_change_closed_accounting_peric
 - 1_03_03_ability_to_delete_used_accounts
 - 1_03_04_logical_access_password
 - 1_04_01_decentralized
 - 1_04_02_disparate_non-integrated
 - 1_04_03_too_complex
 - 1_04_04_inadequate_to_support_business_process
 - 1_04_05_other_design_IT_issues
 - 1_05_01_spreadsheets
 - 1_06_01_outsourcing
 - 1_07_01_masterfiles
 - 1_07_02_computer_data_integrity
 - 1_08_01_staffing
 - 1_08_02_training

DOCUMENTS:

DOCUMENT

Treubacht MS

CODE: 0 1 2 3 4 5 6 7 8 9 10 11

2) Inadequate Reviews: In certain instances, the Company's personnel, at both U.S. and foreign operations, did not perform adequate independent review of reconciliations and other processes.

3) Inadequate Financial Information Systems: The Company's world-wide financial information systems were not integrated and contained many manual processes that may prevent the Company from meeting regulatory filing requirements on a timely and accurate basis. The Company has also identified information technology control weaknesses in the areas of information security, end-user computing, systems program development and change controls.

These material weaknesses were considered in determining the nature, timing and extent of audit tests applied in our audit of the December 31, 2008 consolidated financial statements and financial statement schedule, and this report does not affect our report dated March 16, 2009.

In our opinion, because of the effect of the material weaknesses described above on the achievement of the objectives of the control criteria, American Apparel, Inc. has not maintained effective internal control over financial reporting as of December 31, 2008, based on criteria established in Internal Control-Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission.

We have also audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the consolidated balance sheets as of December 31, 2008 and 2007

- 1_04_02_disparate_non-integrated
- 1_04_04_inadequate_to_support_business_p
- 1_00_01_IT_sentence
- 1_11_03_inadequate_development_mainl
- 1_13_01_security(network, etc.)
- 1_11_01_program_change_testing_a
- 1_00_01_IT_sentence
- 1_05_01_spreadsheets

Fig. 7. Computer-assisted ITW coding using QDA Miner 3.0.4.

these 90 reports, resulting in a population of 387 reports.¹⁰ The failure to detect any ITWs in 28 of these 387 reports, represents a 7% Type 2 error rate for ITW detection at the SOX 404 report level: In nine of these 28 instances, auditors explicitly noted ITWs without describing the nature of the ITW, whereas in the remaining 19 instances, auditors described control weaknesses with words that do not make clear whether or not the weakness is related to an automated portion of the accounting system. To estimate the corresponding Type 1 error we also drew a random sample of 30 reports from the 1621 reports which *Audit Analytics* coded as not having any ITWs but having other control weaknesses (non-ITWs) and applied our automated content analysis procedures to this data, finding a 7% Type 1 error rate (false positive).¹¹

4.2. Result of step 2: developing the dictionary and search criteria

Using frequency reporting features of the qualitative data analysis software, we find that of the over 5000 different words used by auditors in SOX 404 reports, approximately 200 keywords/phrases are included by auditors in their descriptions of ITW concepts. Table 1 reports the frequency with which each keyword/phrase occurs in SOX 404 reports with ITWs in the period of our study.

4.3. Result of step 3: assignment of keywords/phrases to categories

Table 1 shows the keywords/phrases for the 14 categories we identified by using an inductive approach made possible with qualitative data analysis software tools. The 14 categories, in order of decreasing frequency of occurrence are: (1) access, (2) monitoring, (3) design issues, (4) change and development, (5) end-user computing, (6) segregation of incompatible functions, (7) policies, (8) documentation, (9) masterfiles, (10) backup, (11) staffing sufficiency and competency, (12) security (other than over access), (13) outsourcing and (14) operations.

In Table 2, we calculated pairwise associations between each ITW and other ITWs. As the results of Table 2 show, the pairwise associations between ITWs indicate that they are co-reported frequently. From 2004 to 2009, almost half of the possible pairwise associations (35 of 73) between cells with expected cell counts that are large enough to permit statistical inference are positive and significant at $p < 0.05$. Six of the ITWs (Access, Monitoring, Design issues, Changes and development, Policies, and Staffing sufficiency and competency) are associated positively and significantly ($p < 0.05$) with six or more of the other 13 ITWs. All correlation coefficients are less than 0.4 indicating that, although ITWs are co-reported frequently, the 14 categories represent different ITWs.

4.4. Result of step 4: validating dictionary and search criteria

The two audit professionals who reviewed the categorized dictionary suggested no substantive changes to the dictionary. We compared our manual and automated coding of ITWs at the *individual* ITW level under several search criteria, three of which are reported in Table 3. One rule checked for IT weakness keywords/phrases anywhere in the same sentence as IT identifiers, whereas another rule searched only near (in the same sentence and within 20 words) of IT indicators. The latter search strategy is a narrower search that finds fewer false positives but more false negatives than the former. More complex search rules were used to exclude certain terms when other terms are present. Assuming that our manual coding of 1238 ITWs in the 387 reports is 100% reliable, we find that the overall Type 1 and

¹⁰ Until mid-2007 auditors were required to evaluate and opine on management's evaluation process and the control weakness descriptions in management and auditors' reports were usually similar, if not identical. Following the PCAOB acknowledgment that "at times, the related [audit] effort has appeared greater than necessary" and the elimination of the requirement to assess managements' evaluative process (May 24, 2007 PCAOB news release www.pcaob.com), differences in control weakness descriptions in management and auditor reports became more frequent. Audit Analytics codes auditors' reports as IT weak if the management report details ITWs or references software remediation as auditors reports include the phrase "as described in management's report" in their descriptions of internal control weaknesses.

¹¹ In one case, the misidentification was triggered by the word "software" in the company name. In the other case, accounting for "software license revenue" was the trigger. However, the search also found one company which reported "issues in implementing the company's new tax accounting system" that we would classify as an ITW but *Audit Analytics* did not.

Table 2

Significant pairwise associations between information technology weaknesses (ITWs) in reports with ITWs. Table entries are Spearman correlation coefficients (387 reports for 2004–2009).

	Access	Monitoring	Design issues	Change and development	End-user computing	Segregation of incompatible functions	Policies	Documentation	Masterfiles	Backup	Staffing sufficiency and competency	Security (other than over access)	Outsourcing	Operations
Access	1.000	0.234***	0.136**	0.226***	0.049	0.345***	0.186***	0.050	0.074	0.161**	0.105*	0.123*	0.098	0.104*
Monitoring	0.234***	1.000	0.178***	0.113*	0.141**	0.247***	0.250***	0.133**	0.093	0.036	0.159**	−0.010	0.062	0.018
Design issues	0.136**	0.178***	1.000	0.184***	0.203***	0.063	0.101*	−0.010	0.064	−0.038	0.198***	0.020	0.048	0.043
Change and development	0.226***	0.113*	0.184***	1.000	0.071	0.130*	0.185***	0.177***	0.069	0.098	0.241***	0.043	0.097	0.238***
End-user computing	0.049	0.141**	0.203***	0.071	1.000	−0.040	0.130*	0.013	−0.042	−0.043	0.015	−0.005	0.085	0.031
Segregation	0.345***	0.247***	0.063	0.130*	−0.040	1.000	0.123*	0.067	0.137**	0.021	0.102*	−0.002	−0.037	0.102*
Policies	0.186***	0.250***	0.101*	0.185***	0.130*	0.123*	1.000	0.042	0.009	0.237***	0.173**	0.173**	0.098	a
Documentation	0.050	0.133**	−0.010	0.177***	0.013	0.067	0.042	1.000	0.148**	0.104*	0.073	0.073	a	a
Masterfiles	0.074	0.093	0.064	0.069	−0.042	0.137**	0.009	0.148**	1.000	a	a	a	a	a
Backup	0.161**	0.036	−0.038	0.098	−0.043	0.021	0.237***	0.104*	a	1.000	a	a	a	a
Staffing	0.105*	0.159**	0.198***	0.241***	0.015	0.102*	0.173**	0.073	a	a	1.000	a	a	a
Security	0.123*	−0.010	0.020	0.043	−0.005	−0.002	0.173**	0.073	a	a	a	1.000	a	a
Outsourcing	0.098	0.062	0.048	0.097	0.085	−0.037	0.098	a	a	a	a	a	1.000	a
Operations	0.104*	0.018	0.043	0.238***	0.031	0.102*	a	a	a	a	a	a	a	1.000

Table 1 itemizes the ITW weakness indicator keywords/phrases and the IT indicators (shown in bold) used by the automated content analysis to identify ITWs based on searching for ITW weakness indicators in sentences that contain IT indicators near (within 20 words) IT indicators.

Bold text indicates (two-tailed) significance of at least 0.05.

An "a" indicates the expected cell count is too low for meaningful statistical inference.

* Correlation is significant at the 0.1 level (two-tailed).

** Correlation is significant at the 0.01 level (two-tailed).

*** Correlation is significant at the <0.001 level (two-tailed).

Type 2 error rates of this comparison range from 11.6% to 23.9% depending upon which of the three automated search criteria reported in Table 3 Panel A are used: the percentage of Type 1 errors is greatest when the least restrictive search criteria are used (searching for IT weakness keywords/phrases in any sentence containing IT indicator words/phrases), whereas the percentage of Type 2 errors is greatest when the more restrictive search criteria are used (IT weakness keywords/phrases are ignored if they fall within 20 words of the exclusion words/phrases listed in Table 1). The manual coding performed by two coders and the automated coding were identical for over 90% of all 5418 codings (14 codes in 387 reports) under all three search criteria. Table 3 Panel B shows Type 1 and Type 2 error rates, expressed as a percentage of the number of manually identified ITWs, for the 14 ITWs. Regardless of which of the three search criteria are used there is over 80% agreement between the automated and manual coding in the 387 reports for all 14 ITWs (Table 3 Panel B). As shown in Table 3 Panel A, when agreement is judged based on matching of *all* ITW codes in a report, the agreement rate in the 387 reports is approximately 40%. In other words, approximately 40% of the reports were coded identically by manual and automated coding while 60% had one or more differences. In preparing Tables 1, 2, 4, and 5 we report results using the criteria that searches for IT weakness keywords/phrases within 20 words of IT indicators within sentences with IT indicators, the criteria of the three for which the difference between the overall Type 1 and Type 2 error rates minimized (Table 3 Panel A).

4.5. Research question 1 findings

As shown in Table 3 Panel B, the over 80% agreement between our manual and automated coding at the individual ITW level compares favorably to the inter-rater coding reliability reported by Klamm and Weidenmier Watson (2009), the only study of which we are aware that reports inter-rater ITW coding reliability (i.e., 79% for the authors and 73% for coding by an independent third party). Table 4 compares the ITW reporting frequency of our automated content analysis to the frequencies of the 17 IT-related material weaknesses reported by Klamm and Weidenmier Watson (2009) for the first year of SOX 404 reporting (November 23, 2004 through November 24, 2005). When categories relate to weaknesses that are described with very specific IT terminology, frequencies were similar between the studies. For example, Klamm and Weidenmier Watson (2009) reported frequencies for the first year of SOX reporting for “logical access issues” and “spreadsheet issues” (respectively, 55.8% and 24.8%) similar to those that we report for Access and End-user computing ITWs (respectively, 61.4% and 24.2%) in Table 4.

We are able to modify the keywords/phrases in the dictionary used for automated content analysis to explore differences in frequencies between the automated searches and Klamm and Weidenmier Watson (2009) coding. For example, if we limit our automated search to keyword “train*” we identify 5.3% of first year of SOX reporting reports with training issues, a frequency close to the 6.2% that Klamm and Weidenmier Watson (2009) report. Similarly, Klamm and Weidenmier Watson (2009) code less than half as many reports with “explicitly reported: weak IT monitoring” as the automated searches find when searching for both explicit keywords (i.e., “monitor*” and “oversight”) and the other Monitoring category keywords listed in Table 1 (e.g. “review”). However, when we limit the automated analysis to the explicit keywords, “monitor*” and “oversight”, the automated analysis and Klamm and Weidenmier Watson (2009) coding differ by less than 5%. We do not include categories in the dictionary for COSO framework components as we are interested in auditors’ descriptions of *specific* ITWs. However, given we already had a dictionary and search rules to look for words near IT indicators, we leveraged this search capability and searched for explicit use of the terms “control environment”, “risk assessment”, “control activities” and “information and communication” in first year SOX reports and report. The results of these searches are also reported in Table 4.

4.6. Research question 2 findings

Table 5 shows the reporting frequency of ITWs we identified using both manual and automated content analyses with a categorized dictionary in which 14 ITW categories were determined using an inductive approach that began with the actual words used by auditors to describe the ITWs in SOX 404 reports. Table 5 also reports descriptive statistics for both manual and automated searches. The median number of ITWs in all reports is 3, which is the same for both manual and automated approaches.

Table 3

Comparison of information technology weaknesses (ITWs) identification: automated vs. manual coding.

Panel A: Descriptive statistics													
Search method and criteria	Manual search	Automated search: used to report results in Tables				Automated search: more restrictive criteria				Automated search: less restrictive criteria			
		ITW indicator keyword/phrase, within 20 words of an IT indicator ^a				ITW indicator keyword/phrase ignored if within 20 words of exclusion keywords/phrases ^b				ITW indicator keyword/phrase anywhere in a sentence with an IT indicator ^a			
Information technology weaknesses (ITWs)	Manually identified ITWs	Automated-search-identified ITWs	Coding agreement	Type I error(s)	Type II error(s)	Automated-search-identified ITWs	Coding agreement	Type I error(s)	Type II error(s)	Automated-search-identified ITWs	Coding agreement	Type I error(s)	Type II error(s)
At individual ITW level													
14 ITWs in 387 reports in which ITWs are expected (5418 possible codes)													
Number out of 5418 possible codes	1238	1255	5009	213	196	1126	4992	157	269	1358	4984	277	157
% of 5418 possible codes	22.8%	23.2%	92.5%	3.9%	3.6%	20.8%	92.1%	2.9%	5.0%	25.1%	92.0%	5.1%	2.9%
% of manually coded ITWs	n/a	n/a	n/a	17.2%	15.8%	n/a	n/a	13.9%	23.9%	n/a	n/a	20.4%	11.6%
Minimum number per report	0	0	7	0	0	0	7	0	0	0	7	0	0
Maximum number per report	10	11	14	5	6	9	14	5	6	11	14	5	6
Median number per report	3	3	13	0	0	2	13	0	0	3	13	0	0
Mean number per report	3.20	3.24	12.94	0.55	0.51	2.91	12.90	0.41	0.70	3.51	12.88	0.72	0.41
Standard deviation	2.14	2.20	1.22	0.90	0.83	2.10	1.24	0.71	1.03	2.28	1.28	1.04	0.76
At SOX 404 report level													
in 387 reports in which ITWs are expected													
Number of reports out of 387	373	354	158	143	137	340	152	119	170	359	155	166	112
% of 387 reports	96.4%	91.5%	40.8%	37.0%	35.4%	87.9%	39.3%	30.7%	43.9%	92.8%	40.1%	42.9%	28.9%

Panel B: Type I and Type II errors for 14 ITWs identified with automated content analysis

Search method and criteria	Manual search	Automated search: used to report results in Tables				Automated search: more restrictive criteria				Automated search: less restrictive criteria			
		ITW indicator keyword/phrase, within 20 words of an IT indicator ^a				ITW indicator keyword/phrase ignored if within 20 words of exclusion keywords/phrases ^b				ITW indicator keyword/phrase anywhere in a sentence with an IT indicator ^a			
	Number of ITWs	Number of ITWs	Errors as percentage of manually identified ITWs		Coding agreement	Number of ITWs	Errors as percentage of manually identified ITWs		Coding agreement	Number of ITWs	Errors as percentage of manually identified ITWs		Coding agreement
	Manually identified	Automated-search-identified	Type I error(s) (% of ITWs)	Type II error(s) (% of ITWs)	% of 387 reports	Number of ITWs	Type I errors (% of ITWs)	Type II errors (% of ITWs)	% of 387 reports	Number of ITWs	Type I errors (% of ITWs)	Type II errors (% of ITWs)	% of 387 reports
Information technology weaknesses (ITWs)													
Access	224	211	1%	7%	96%	201	1%	11%	93%	211	1%	7%	96%
Monitoring	171	188	20%	10%	87%	174	18%	16%	85%	201	27%	9%	84%
Design issues	145	133	18%	26%	83%	118	14%	33%	82%	146	21%	21%	84%
Change and development	125	131	20%	15%	89%	120	16%	20%	88%	138	24%	14%	88%
End-user computing	121	124	3%	1%	99%	121	3%	3%	98%	124	3%	1%	99%
Segregation	131	110	5%	21%	91%	107	5%	24%	90%	125	9%	14%	92%
Policies	67	88	57%	25%	86%	57	28%	43%	88%	110	75%	10%	85%
Documentation	54	72	50%	17%	91%	52	30%	33%	91%	85	70%	13%	88%
Masterfiles	64	55	8%	22%	95%	51	5%	25%	95%	55	8%	22%	95%
Backup	36	35	14%	17%	97%	32	14%	25%	96%	35	14%	17%	97%
Staffing and competency	36	32	25%	36%	94%	29	25%	44%	94%	52	64%	19%	92%
Security (other than access)	30	32	43%	37%	94%	25	23%	40%	95%	32	43%	37%	94%
Outsource	15	23	73%	20%	96%	23	73%	20%	96%	23	73%	20%	96%
Operations	19	21	37%	26%	97%	16	11%	26%	98%	21	37%	26%	97%

^a Table 1 itemizes the ITW weakness indicator keywords/phrases and the IT indicators (shown in bold) used by the automated content analysis to identify ITWs. The results presented in Tables 1, 2, 4, and 5 are based on searching for ITW weakness indicators in sentences that contain IT indicators near (within 20 words) IT indicators. The last four columns of this table show how results would differ when the nearness constraint is relaxed.

^b The columns shown under the “more restrictive criteria” heading, show how results would differ if ITWs that occur within 20 words, in the same sentence, as an IT indicator^a are ignored if also within 20 words (as determined by the QDA content analysis software) of “exclusion keyword/phrases”. Exclusion keyword(s)/phras(es), frequently associated with SOX 404 “boilerplate” definitions and non-ITW contexts are listed in Table 1.

We used the frequency reporting feature of the content analysis software to check whether or not auditors frequently used COSO components, COBIT domains or broad categories of “general IT controls” and “application controls” terminology for categories. Consistent with [Klamm and Weidenmier Watson \(2009\)](#) and [Gupta \(2006\)](#), we found that COSO component names, other than monitoring, were infrequently used in SOX 404 reports in sentences containing an IT indicator word/phrase: specifically (i) “risk assessment” (10 reports), (ii) “control environment” (54), (iii) “information and communication” (9), and (iv) “control activities” (10). Furthermore, the four COBIT 4.1 domains (“plan and organize”, “acquire and implement”, “deliver and support” and “monitor and evaluate”) are not referenced at all. The phrase “general controls” (and synonymous phrases “general computer controls”, “general computing controls”, “IT general controls”, and “ITGC”) was used in less than 14% (54) of the reports and in all but five of these 54 reports other ITW identifiers were also present. The phrase “application control(s)” was used in less than 4% (17) of the reports.

Some SOX 404 reports refer to specific applications (e.g., inventory and payroll systems) that are, or are likely to be, affected by the reported ITWs. Other reports either do not refer to applications in describing ITWs or use general terms such as “certain” or “various” to refer to applications without explicitly naming the applications affected. Not only are descriptive labels such as “general controls” used infrequently in SOX 404 reports, but also, as shown in [Table 5](#), approximately 30% of IT-weak reports (132 out of 387) reference specific financial applications in sentences which we search for ITW descriptions. [Table 5](#) compares the frequency of ITWs in all reports in which we expected to find ITWs to the frequencies in reports in which auditors use keywords associated with financial applications and COSO components (other than

Table 4

Percentages of firms reporting information technology weaknesses (ITWs): first year of SOX 404 reports.

Automated content analysis		Klamm and Weidenmier Watson (2009)	
Identified using automated content analysis ^a of 132 IT-Weak auditors' SOX 404 reports		Identified by Klamm and Weidenmier Watson (2009) using manual content analysis of 129 IT-Weak managements' SOX 404 reports	
ITWS			
Access	61.4%	Logical access	55.8%
Monitoring	56.1% ^b	Explicitly reported: weak IT monitoring	25.6%
Change and development	38.6%	Program change control issues	28.7%
		Coding/program errors	7.0%
Segregation	37.1%		
Design issues	36.4% ^c	Disparate, non-integrated systems	8.5%
		Functionally complex	4.7%
		Decentralized systems	3.1%
End-user computing	24.2%	Spreadsheet	24.8%
Documentation	24.2%	Lack of systems documentation	16.3%
Policies	22.7%		
Masterfiles	20.5%		
Staffing and competency	11.4% ^d	Systems training	6.2%
Backup	10.6%	Ineffective or lack of disaster recovery plan	7.0%
Security	9.8%	Security issues	15.5%
Outsource	8.3%		
Operations	6.8%		
		Other IT control activities issues	50.4%
Additional searches ^a			
“control environment”	15.9%	Explicitly reported: weak IT control environment	15.5%
“risk assessment”	5.3%	Explicitly reported: weak IT risk assessment	2.3%
“control activities”	4.5%	Explicitly reported: weak IT control activities	14.0%
“information and communication”	3.8%	Explicitly reported: weak IT information and communication	6.2%

^a [Table 1](#) itemizes the ITW weakness indicator keywords/phrases and the IT indicators used by the automated content analysis to identify ITWs based on searching for ITW weakness indicators in sentences in auditors' SOX 404 reports that contain IT indicators near (within 20 words) IT indicators.

^b The frequency is 31.1% if only keywords “monitor” and “oversight” are used to search for Monitoring ITWs.

^c The frequency is 18.2% if the keyword “design”, which also refers to the design of manual controls, is omitted from automated searches for Design ITWs.

^d The frequency is 5.3% if only the keyword “train” is used to search for Staffing and competency ITWs.

Table 5Information technology weaknesses (ITWs) reported in auditors' SOX 404 reports 2004–2009^a.

Search within 20 words of IT indicator in sentences with IT indicators:content analysis method	Search 1				Search 2				Search 3				Frequency comparison (manual counts)	
	All reports in which ITWs are expected ^a				Sample of reports that include both IT and financial application keywords ^b				Sample of reports that include both IT and COSO component (other than monitoring) keywords ^c					
	Manual		Automated		Manual		Automated		Manual		Automated		p values	
Information technology weaknesses (ITWs)	n	% of reports	n	% of reports	n	% of reports	n	% of reports	n	% of reports	n	% of reports	Search 2 vs. Search 1	Search 3 vs. Search 1
Access	224	58%	211	55%	85	64%	81	61%	44	73%	43	72%		*
Monitoring	171	44%	188	49%*	72	55%	78	59%	34	57%	42	70%*	*	*
Design issues	145	37%	133	34%	58	44%	54	41%	30	50%	30	50%		*
Change and development	125	32%	131	34%	57	43%	63	48%	29	48%	29	48%	**	**
End-user computing	121	31%	124	32%	53	40%	54	41%	27	45%	27	45%	*	*
Segregation	131	34%	110	28%*	52	39%	44	33%	24	40%	25	42%		
Policies	67	17%	88	23%**	19	14%	39	30% ^d	20	33%	30	50% ^d	d	d
Documentation	54	14%	72	19%**	21	16%	26	20% ^d	15	25%	18	30% ^d	d	d
Masterfiles	64	17%	55	14%	34	26%	31	23% ^d	8	13%	9	15% ^d	d	d
Backup	36	9%	35	9% ^d	12	9%	13	10% ^d	6	10%	6	10% ^d	d	d
Staffing and competency	36	9%	32	9% ^d	12	9%	12	9% ^d	13	22%	14	23% ^d	d	d
Security (other than access)	30	8%	32	8% ^d	7	5%	7	5% ^d	8	13%	5	8% ^d	d	d
Outsource	15	4%	23	4% ^d	10	8%	14	11% ^d	3	5%	5	8% ^d	d	d
Operations	19	5%	21	5% ^d	4	3%	9	7% ^d	6	10%	7	12% ^d	d	d
Total number of ITWs	1238		1255		496		525		267		290			
Number of reports	387		387		132		132		60		60			
Mean number of ITWs	3.20		3.24		3.76		3.98		4.45		4.83			
Standard deviation	2.14		2.20		2.39		2.44		2.65		2.53			
Skewness	0.81		0.69		0.48		0.33		0.05		−1.30			
Minimum number of ITWs	0		0		0		0		0		0			
Maximum number of ITWs	10		11		10		11		10		11			
Median number of ITWs	3		3		4		4		5		5			

^a Compares the number of ITWs identified and the frequency of reporting using manual (computer assisted) vs. automated content analysis for all auditors SOX 404 reports, a subsample of reports in which financial applications are referenced^b, and a subsample of reports in which the COSO framework is referenced^c.

^b Reports in which automated content analysis identified financial applications keywords (i.e. Accounts Payable, Accounts Receivable, Accrued Liabilities, Cash, Capital Assets, Cost of Goods, Cost of Sales, Fixed Assets, Inventory, Payroll, Sales, and Taxes) within a sentence with an IT indicator (Table 1).

^c Reports in which automated content analysis identified COSO related keywords (except Monitoring) (i.e., Control Activities, Control Environment, Information and Communication, and Risk Assessment) within a sentence with an IT indicator (Table 1).

^d Expected cell counts too low for statistical inference of binomial test of proportion comparing proportion of manually to automated identified ITWs.

* Difference in proportion of reports is significant at the $p < .05$ level.

** Difference in proportion of reports is significant at the $p < .01$ level.

*** Difference in proportion of reports is significant at the $p < .001$ level.

monitoring) in sentences we search for ITW descriptions. Monitoring, change and development, and end-user computing ITWs, representing half of the six ITWs where counts are sufficient for statistical analysis, occur more frequently ($p < 0.05$) in reports in which auditors reference specific applications than in the population of all 387 IT-weak reports.¹² Further, while COSO components (other than monitoring) are referenced in the same sentence as IT indicators in only 60 of the 387 IT-weak reports, five of the ITWs where counts are sufficient for statistical analysis (Access, Monitoring, Design issues, Change and development, End-user computing, and Segregation) occur more frequently ($p < 0.05$) in reports in which auditors refer to components of the COSO framework (Table 5) than in the population of IT-weak reports. The median number of ITWs is greater in reports that refer to financial applications (4 vs. 3 in all reports coded as having ITWs) and COSO components (5 vs. 3 in all reports coded as having ITWs).

5. Discussion

Methodologically, this study demonstrates the advantages and limitations of using content analysis software in the study of narrative reports on the effectiveness of IT internal control. Until now, other researchers who have used SOX 404 reports to study ITWs have relied on the single code in *Audit Analytics* to identify the presence of ITWs or have identified specific categories of ITWs through an arduous manual process. The resource demands of relying on experts to visually scan and identify ITWs in text data sources impact on research design decisions and represent an obstacle both to reliably link the presence of specific categories of ITWs with other variables – such as financial performance, audit fees, and governance – and to implications of those associations. In addition to providing a categorized dictionary that may be used in ITW research, this study outlines techniques that may be used to develop an automated content analysis approach for analysis of unstructured text in other contexts.

Research questions, data sources, coding expertise, coders' time, and coders' expertise with qualitative data analysis software will determine the coding approach best suited to the coding task. In this study we demonstrated the use of sophisticated search rules and a multi-level categorized dictionary. However, it is possible that less sophisticated automated content analysis strategies, in combination with manual content analysis, will suffice for other studies. For example, 71% (276 of the 387) of the reports with ITWs analyzed in this study would have been located with a simple search of auditor's SOX 404 reports for any of five most frequently occurring IT identifiers (i.e., information technology, spreadsheet*, software, financial application*, and information system*). Manual coding efforts may be reduced by using such simple searches to locate portions of unstructured text to which manual content analysis may subsequently be applied. When selecting content analysis strategies, researchers should consider not only the challenges of implementing an automated approach (i.e., creating and validating dictionaries and search rules), but also the comparative advantages of effectively automating the content analysis process (the gains in consistency, scalability, replicability and transparency). Dictionaries are re-usable. Hence, potential future studies, as well as the immediate research project, should factor into decisions about which tools/techniques to use on the continuum from manual to automated content analysis depicted in Fig. 1.

Our study extends prior research that has studied ITWs at a detailed level (e.g., Bell et al., 1998; Messier et al., 2004; Hammersley et al., 2008; Klamm and Weidenmier Watson, 2009). The dictionary and search criteria that we have created to identify and categorize reported ITWs enable users to perform consistent, transparent, replicable,¹³ affordable and scalable ITW identification in SOX 404 reports. Furthermore, this dictionary of words/phrases provides a snapshot of IT-related terminology actually used by auditors and may assist development of text analysis approaches to facilitate the study of IT controls in SOX 404 reports and other disclosures in the U.S. and other jurisdictions. The content analysis of auditors' reports using our dictionary identified the following 14 categories of material IT weaknesses, in order of decreasing frequency of occurrence: (1) access, (2) monitoring, (3) design issues, (4) change and development, (5) end-user computing, (6) segregation of incompatible functions, (7) policies, (8) documentation, (9) masterfiles,

¹² The proportion of ITWs referencing applications is based on the manual coding of ITWs used to validate the dictionary as described in Step 4 of Section 3.

¹³ Such replication may be impacted by retroactive database updates that *Audit Analytics* makes in studies that rely on *Audit Analytics* coding to identify IT weak reports in which to search for ITWs. We extracted 2004–2008 data and SOX 404 reports from the *Audit Analytics* database on November 2, 2009 and the 2009 data and reports on July 26, 2010.

(10) backup, (11) staffing sufficiency and competency, (12) security (other than over access), (13) outsourcing and (14) operations. These 14 categories were determined adopting a unique, bottom-up, inductive approach to ITW identification and categorization that would not have been feasible without frequency reporting, keyword-in-content, keyword retrieval, and other automated content analysis software tools.

We find that automated ITW identification using a dictionary based on auditors' actual words in SOX 404 reports categorizes ITWs differently than manual grouping based on professional standards and other guidance such as the COSO framework. An explanation for such differences may be the nature of the negotiation process between auditors and management. [Bedard and Graham \(2011\)](#) find that auditors judge control deficiencies as more severe, and hence more likely to be reported in SOX 404 reports, if a misstatement is detected. [Bell et al. \(1998: 38\)](#)¹⁴ find few audit differences attributed to general control failures (e.g., hardware failure, documentation). Accordingly, references to applications and the less frequent reporting of ITWs such as Operations, Backup, Security, and Documentation is consistent with a negotiation process that prevents reporting of these weaknesses unless a misstatement is detected. Our finding that half of the ITWs, with counts sufficient for statistical analysis, are reported more frequently when financial applications are mentioned is also consistent with [Bedard and Graham's \(2011\)](#) finding: auditors are likely to use financial application keywords (e.g. "accounts receivable" and "accounts payable") in descriptions of many financial misstatements, keywords that we also used to identify reports referring to financial applications.

However, similar reasoning does not explain why we observed all but one of the ITWs where counts are sufficient for statistical analysis more frequently when COSO components are mentioned than in the population of IT-weak SOX 404 reports. Perhaps ITWs are more likely to be reported when non-ITW are also reported. Also, auditors may use COSO component language to classify control weaknesses in reports where many control weaknesses are reported. Another unexplained observation is that risk assessment controls — one of the five components of the COSO framework — are not identified as being weak in companies reporting numerous material IT weaknesses. Overall, the potential disconnect we observed between published guidance (e.g. COSO) and auditor SOX 404 reporting of ITWs suggests further investigation of these issues, and additional guidance from standard setters and regulators to managers and auditors on the reporting of ITWs, is warranted.

5.1. Limitations and future research

We acknowledge certain limitations of our analyses. First, while we demonstrated the comparative advantages of many features of automated content analysis software, we did not examine the efficacy of using some of the simpler features. For example, we demonstrated the usefulness of advanced searching capabilities, dictionary building tools, and visualization tools (e.g., dendrograms and concept maps) but did not discuss how to use the simpler computer-assisted coding features ([Fig. 1](#)) common to most qualitative data analysis. An extension of this study might be to study the efficacy of using automation, rather than manual methods, to apply codes to selected text, compute inter-rater agreement, and locate coded segments of text in lengthy, unstructured text such as Management's Discussion and Analysis.

Second, the reliability of automated identification of ITWs depends on a number of manual activities including keyword/phrase selection, aggregation of keywords into categories, and creation of search criteria. The reliability of automated text analysis depends not only on the sophistication of the dictionary and search criteria but also on when the "refining" of the dictionary is stopped. As a result, the automated search is not perfect, resulting in both Type 1 and Type 2 errors. Dictionary refinement will always be an on-going process as the dictionary used for automated searching needs to be kept up to date. As [Kuechler \(2007\)](#) observes, such updating, while time-consuming and sometimes tedious, is necessary, especially when there are announcements of changes in authoritative guidance and standards. This research could be extended by studying the incremental benefits of refining dictionaries and search criteria vs. supplementing a less refined automated search with manual coding of automatically identified segments of text.

¹⁴ The data upon which the study is based was collected in 1989 and technology has since changed. [Bell et al. \(1998\)](#) acknowledge this but counter that the results pertain to "general error attributes" and not "specific system attributes".

A third limitation is that the weaknesses that we analyze are only the weaknesses that were reported by the entity's auditor as a result of an audit process that may not identify all material ITWs and a negotiation process with management that is thought to act as a screen ensuring that only the most severe weaknesses are reported (ITGI, 2006; Wolfe et al., 2009). Therefore, the picture of financial reporting systems that these weaknesses portray may not be complete. Adding control deficiencies that were not considered material weaknesses may portray a more complete picture and could represent a valuable extension of this study. Also obtaining information directly from auditors rather than from their reports, such as the Bedard and Graham (2011) and Bell et al. (1998) studies that classify the reasons for the occurrence of both material and immaterial audit differences might provide a more complete picture of actual ITWs.

In addition, the pattern of reported ITWs raises a number of questions for further investigation. For example, access, monitoring, design issues, and change management represent issues that are frequently reported over the six years since SOX 404 reports began to be issued. They therefore represent areas that need to be addressed by managers, auditors, regulators and researchers. Also, end-user computing issues are one of the more frequently reported ITWs. Despite anecdotal evidence of the problems spreadsheet errors create in financial reporting systems (Curtis et al., 2009), there is little research into their prevention and detection (Powell et al., 2008). While spreadsheets may be used less as financial reporting systems' reporting flexibility increases, end user computing issues are likely to continue as the use of cloud computing (e.g. Google Docs) by non-IT personnel increases. Security concerns receive much attention in the practitioner literature, but other than access controls, security is perennially a low ranked ITW, accounting for a marginal number of reported ITWs. Similarly, outsourcing is associated with few reported ITWs. This observation may indicate that outsourced components of financial reporting systems are comparatively well managed.

Also, as previously noted, we searched for but found few references to the categories of IT controls referred to in prominent frameworks, guidelines, and even standards. A potential problem arising from the lack of linkage between the terminology used in the auditors' reports and published guidelines and standards is that users of the internal control reports will find it difficult to link the reported weaknesses back to professional literature and standards so as to interpret the impact of the reported weaknesses on the respective companies, the likely causes of those weaknesses and potential avenues and time horizon for their effective remediation. An extension of our research would be to have users read the auditors' reports and attempt to link the ITWs identified therein to the published frameworks and assess their impact on the company. Another extension would be to perform a more nuanced analysis of the language used in auditors' reports to investigate the ways in which material weaknesses are portrayed. It would also be worth investigating the reasons for the apparent reluctance by managers and auditors to use the headings in frameworks, guidelines, and standards in favor of their own terminologies. Our understanding of internal control would also be furthered by a study of how the individual ITWs are influenced by factors such as time, auditor type, and industry, and the associations of ITWs with non-ITWs and financial misstatements. We are planning to perform such a study as an extension of this research.

Finally, we suggest that an automated content analysis can produce a reliable, transparent and replicable coding of textual information and should be considered in future studies of managements' and auditors' textual communications with stakeholders in place of proprietary coding that may be less reliable, less transparent and less replicable.

References

- Ashbaugh-Skaife H, Collins DW, Kinney WR, LaFond R. The effect of SOX internal control deficiencies and their remediation on accrual quality. *Acc Rev* 2008;83(1):215–50.
- Ashbaugh-Skaife H, Collins DW, Kinney WR, LaFond R. The effect of SOX internal control deficiencies on firm risk and cost of equity. *J Acc Res* 2009;47(1):1–43.
- Bedard JC, Graham L. Archival evidence on detection and severity classification of Sarbanes–Oxley Section 404 internal control deficiencies. *Acc Rev* 2011;86(3):825–55.
- Bell TB, Knechel WR, Payne JL, Willingham JJ. An empirical investigation of the relationship between the computerization of accounting systems and the incidence and size of audit differences. *Audit J Pract Theor* 1998;17(1):13–38.
- Beneish D, Billings M, Hodder L. Internal control weaknesses and information uncertainty. *Acc Rev* 2008;83(3):665–703.
- Boritz E, Lim JH. IT control weaknesses, IT governance and firm performance. Working paper. University of Waterloo; 2008.

- Canada J, Sutton SG, Kuhn Jr JR. The pervasive nature of IT controls: an examination of material weaknesses in IT controls and audit fees. *Int J Acc Inf Manage* 2009;17(1):106–19.
- Cohen D, Dey E, Lys T. Real and accrual-based earnings management in the pre-and post-Sarbanes Oxley periods. *Acc Rev* 2008;83(3):757–87.
- Curtis MB, Jenkins JG, Bedard JC, Deis DR. Auditors' training and proficiency in information systems: a research synthesis. *J Inf Syst* 2009;23(1):79–96.
- Doyle J, Ge W, McVay S. Determinants of weaknesses in internal control over financial reporting. *J Acc Econ* 2007a;44(1/2):193–223.
- Doyle J, Ge W, McVay S. Accruals quality and internal control over financial reporting. *Acc Rev* 2007b;82(5):1141–70.
- Fan W, Wallace L, Rich S, Zhang Z. Tapping the power of text mining. *Commun ACM* 2006;49(9):77–82.
- Fisher IE, Garnsey MR, Goel S, Tam K. The role of text analytics and information retrieval in the accounting domain. *J Emerg Technol Acc* 2010;7:1–24.
- Gupta P, sponsored by the Institute of Management Accountants (IMA). Internal Control COSO 1992 Control Framework and Management Reporting on Internal Control: survey and analysis of implementation practices. Available from the Institute of Management Accountants, 2006.
- Hammersley JS, Myers LA, Shakespeare C. Market reactions to the disclosure of internal control weaknesses and to the characteristics of those weaknesses under Section 302 of the Sarbanes Oxley Act of 2002. *Rev Acc Stud* 2008;13(1):141–65.
- Hoitash R, Hoitash U, Bedard J. Internal controls quality and audit pricing under the Sarbanes–Oxley Act. *Audit J Pract Theor* 2008;27(1):105–26.
- Hoitash R, Hoitash U, Johnstone K. Internal control material weaknesses and CFO compensation. *Contemp Acc Res* forthcoming. Accepted manuscript online: 28 JUN 2011 11:28AM EST | doi:10.1111/j.1911-3846.2011.01122.x.
- Huntton J. Discussant's comments on presentations by John Lainhart and Gerald Trites. *J Inf Syst* 2000;14(S-1):33–6.
- IT Governance Institute. (ITGI). Appendix I sample deficiency evaluation decision tree. IT control objectives for Sarbanes–Oxley: the role of IT in the design and implementation of internal control over financial reporting. 2nd edition. Rolling Meadows, IL: IT Governance Institute; 2006.
- IT Governance Institute. (ITGI). COBIT 4.1. Rolling Meadows, IL: IT Governance Institute; 2007. Available online at <http://www.isaca.org>.
- Jha R, Kobelsky K, Lim JH. The impact of performance-based compensation on internal control. Working paper. Baylor University and University of Waterloo; 2010.
- Klamm BK, Weidenmier Watson M. SOX 404 reported internal control weaknesses: a test of COSO framework components and information technology. *J Inf Syst* 2009;23(2):1–23.
- Krishnan J. Audit committee quality and internal control: an empirical analysis. *Acc Rev* 2005;80(2):649–75.
- Kuechler W. Business applications of unstructured text. *Commun ACM* 2007;50(10):86–93.
- Lacity MD, Janson MA. Understanding qualitative data: a framework of text analysis methods. *J Manage Inf Syst* 1994;11(2):137–56.
- Li C, Peters G, Richardson VJ, Weidenmier Watson M. The Consequences of Information Technology Control Weaknesses on Management Information Systems: The Case of Sarbanes–Oxley Internal Control Reports MIS Q forthcoming.
- Masli A, Richardson VJ, Weidenmier Watson M, Zmud R. CEO, CFO & CIO engagement in information technology management: the disciplinary effects of Sarbanes–Oxley information technology material weaknesses. Working Paper. University of Arkansas; 2009.
- Messier Jr WF, Eilifsen A, Austen LA. Auditor detected misstatements and the effect of information technology. *Int J Audit* 2004;8:223–35.
- Pollach I. Taming textual data: the contribution of corpus linguistics to computer-aided text analysis. *Organ Res Methods* 2011. Published online before print August 15, 2011, doi:10.1177/1094428111417451 *Organizational Research Methods* August 15, 2011 1094428111417451.
- Powell SG, Baker KR, Lawson B. A critical review of the literature on spreadsheet errors. *Decis Support Syst* 2008;46(1):128–38.
- Public Company Accounting Oversight Board (PCAOB). Auditing Standard No. 2 — an audit of internal control over financial reporting that is integrated with an audit of financial statements. Available online at <http://pcaobus.org> 2004.
- Public Company Accounting Oversight Board (PCAOB). Auditing Standard No. 5 — an audit of internal control over financial reporting that is integrated with an audit of financial statements. Available online at <http://pcaobus.org> 2007.
- Raghunandan K, Rama D. SOX Section 404 material weakness disclosures and audit fees. *Audit J Pract Theor* 2006;25(1):99–114.
- Securities and Exchange Commission (SEC). Final rule: management's report on internal control over financial reporting and certification of disclosure in Exchange Act periodic reports. Available online at <http://www.sec.gov/rules/final.shtml> 2003.
- Wolfe CJ, Mauldin EG, Chandler MC. Concede or deny: do management persuasion tactics affect auditor evaluation of internal control deviations? *Acc Rev* 2009;84(6):2013–37.